



G.A.O.

United States General Accounting Office
Washington, DC 20548

Logistics and
Communications
Division

E-163074

MAR 21 1979

The Honorable Harold Brown
The Secretary of Defense

Dear Mr. Secretary:

We have completed our examination of automated systems security programs in the Department of Defense (DOD) and other major Federal agencies. Our efforts resulted in a report, "Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, Jan. 23, 1979). (See enc.)

The January report concludes that agency management attention to programs for protecting data in automated systems was deficient. However, we see potential for improvement if agencies respond aggressively to the Office of Management and Budget (OMB) Circular A-71, TM 1 (Security of Federal Automated Information Systems, July 27, 1978). The report states that these requirements are now being coupled with broader concerns for improving agency controls over fraud and abuse. As you know, the President's December 13, 1978, memorandum to heads of executive departments and agencies requires their personal attention in these areas.

Initially, our review was to include automated systems security programs in selected civil agencies, DOD, and component services. We advised DOD that we would not be directly examining its activities because of its extensive internal audits. Instead, these audits and the implications for security programs of audit findings were assessed.

We identified and analyzed 106 computer security-oriented audits related to over 270 facilities and/or systems. These audits were conducted by the Defense Audit Service, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency. We also reviewed with DOD and component service policy officials the extent of programs and guidelines to protect sensitive data.



007767
110907

LCD-79-109
(941121)
(941145)

Our review of DOD's internal audits and of policy in effect and in development demonstrated that Defense agencies have experienced difficulties in each of the broad areas discussed in our January 1979 report. These include

- management's recognition of the need for comprehensive programs to protect all sensitive data,
- clarification of policies and regulations to define the scope of security programs and responsibilities,
- independence of system security administration from computer operations,
- application of risk management techniques,
- compliance with security requirements, and
- enhancement of technical capabilities of internal audit organizations to perform automated systems reviews.

During our review we were pleased to find that the Department of the Army, anticipating the objectives of OMB Circular A-71, has issued Army Regulation 380-380 prescribing policies and procedures for automated systems security. This regulation provides the framework for a program that we feel addresses the problems discussed in our January 1979 report. We hope that DOD will develop a program that will encourage and accelerate similar initiatives in other DOD components.

In this regard, a focal point is needed to develop a comprehensive DOD automated systems security program and to issue written guidance. DOD may wish to establish this responsibility in the Director of Information Security, Office of the Deputy Assistant Secretary for Administration. This office meets the requirement of the recommendation in our January report for independence from automated data processing operations. Moreover, it is responsible for directing the protection of national security data.

We briefed personnel of the Defense Audit Service, Army Audit Agency, Naval Audit Service, and the Air Force Audit Agency and provided them with the results of our

analysis of their audits. We commend these Defense agencies for their significant level of effort in security-oriented audits.

The joint DOD audit agencies' study group, under the leadership of ODBSD (Audit), Audit Policy, recently assessed and reported on automatic data processing audit performance, skills, and training. As an outcome of the study, audit guidelines have been proposed for adoption throughout DOD. This should further encourage (1) enhancement of audit staff qualifications and training and (2) more comprehensive audits of information systems and systems development efforts.

We believe that continuing these efforts could, to a significant degree, satisfy our January report recommendation on audit of systems security. DOD may wish to consider continuing such a group as a permanent basis for coordinating and developing additional audit guidelines and approaches to auditing data security programs and systems controls.

We stated in our January report that our work in DOD, ongoing at the time the report was issued, showed its component agencies were experiencing problems in each of the areas addressed. The report was transmitted to your office by the Comptroller General's circular letter which highlighted the report's findings and recommendations for the heads of all Federal agencies and departments.

Section 236 of the Legislative Reorganization Act of 1970 requires the head of a Federal agency to submit a written statement on actions taken on our recommendations to select congressional committees. In view of OMB's current role of promoting and coordinating agency efforts in developing automated systems security programs, we requested that OMB review agency responses to our report recommendations addressed to all executive agency heads. We also requested that OMB provide a consolidated response for all agencies. Therefore, DOD should respond to OMB on the recommendations in the January report.

We appreciate the cooperation extended us in our review. We would gladly discuss with your representatives efforts underway in your agency to respond to our report and the related executive branch requirements. You may contact either

163074

Mr. Robert Gilroy, Assistant Director, Logistics and Communications Division, or Mr. Ernest Cooper, Audit Manager for this assignment on (202) 275-6531.

A copy of this letter is being sent, pursuant to his request for an examination of the status and effectiveness of computer security in major Federal agencies, to the Chairman, Subcommittee on Government Information and Individual Rights, House Committee on Government Operations. Copies are also being sent to the Chairmen, House Committee on Government Operations, the Senate Committee on Governmental Affairs, the House and Senate Committees on Appropriations, and the Director, Office of Management and Budget.

Sincerely yours,



R. W. Gutmann
Director

Enclosure